ARIZONA DEPARTMENT OF ADMINISTRATION - ASET

Arizona FirstNet

Response to: NTIA / FirstNet Responder Network Authority Further Proposed Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012 – Third Notice 2015-10140

6/4/2015

The responses in this document are a compendium of comments of public safety and public service Stakeholders in the State of Arizona representing a diverse blend of disciplines and geographies. The responses may be paraphrased to more clearly reflect the intent of the Stakeholder comment.

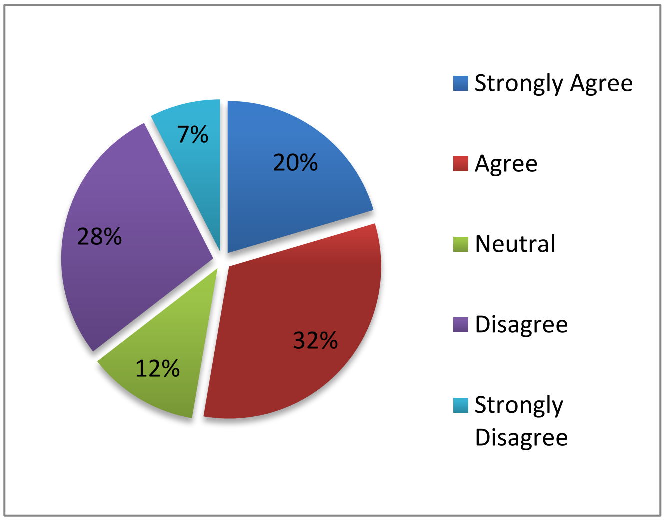
They do not represent a legal opinion or official policy position of the State.

Arizona stakeholders were mixed on the issue of allowing access to only entire organizations versus a public safety subset of an organization. They were generally open to allowing either infrequent or non-traditional public safety agencies on the NPSBN.

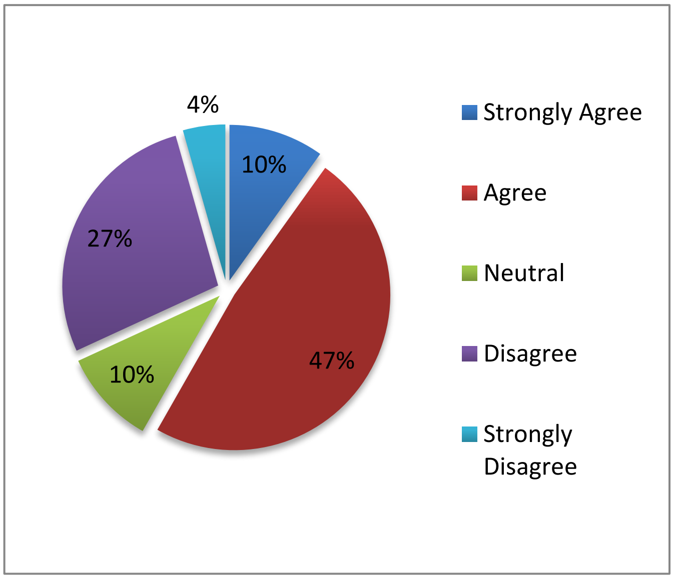
With respect to M2M usage, most agreed that sensors/data feeds that were directly related to public safety metrics and owned by governmental/utility should be allowed on the NPSBN, however there were concerns about the explosive growth of those devices and possible impacts on network bandwidth.

Regarding the possibility that certain entities may be allowed in one state but not in another and what would happen if cross border mutual aid were required, most felt that MOUs, IGAs or national level interoperability should supersede the state rules and access should be allowed. In other words, the needs of the incident should prevail.

1. **An "entity" should be defined as a group or authority of a certain minimum size or nature (such as an entire government agency or department)**

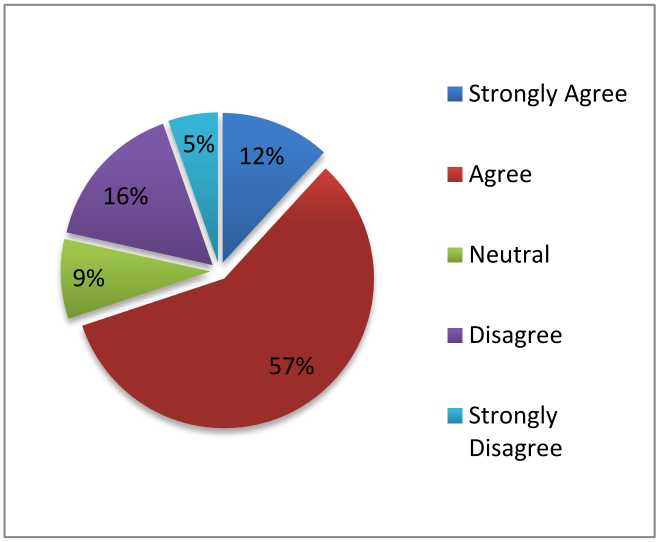


2. **An "entity" could include only a sub-group or an individual from an organization or agency (part of an organization or agency)**

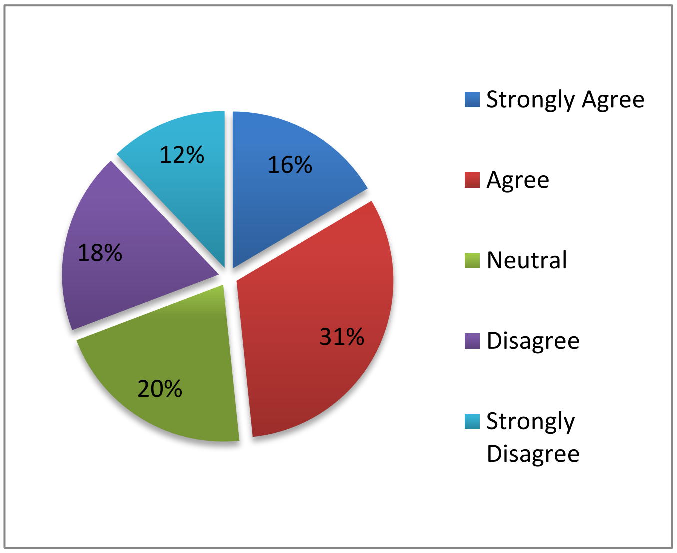


The example provided by in the notice has been echoed by our stakeholders during meetings, indicating that an emergency room in the hospital due to interactions with firefighters on medical calls should be on the network. In addition, we have heard from organizations such as Boeing and Raytheon that have their own fire departments that need on the network.

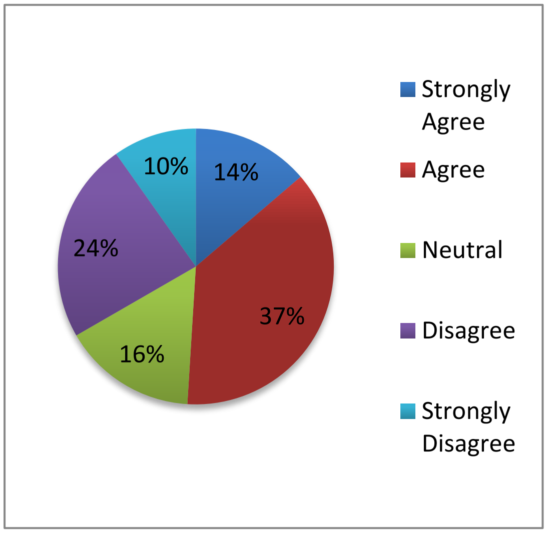
3. **An organization or agency that provides public safety services some, but not all the time, can qualify as a public safety entity (part-time public safety)**



4. **An organization or agency that provides services close or related to, but not identical to traditional public safety services can qualify as a public safety entity (support of public safety)**



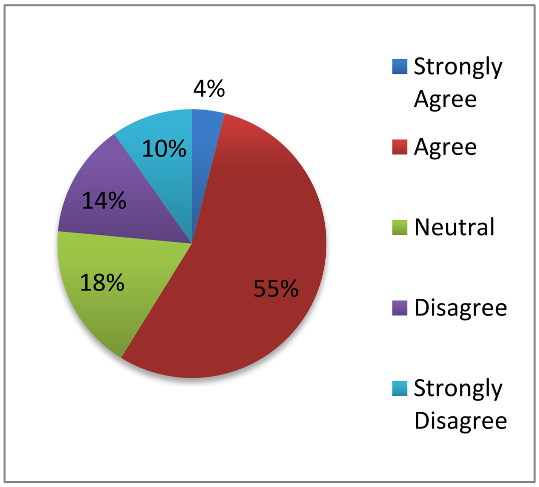
5. "Things" that perform a public safety function should be considered eligible to use the FirstNet network, even if they are not operated by a public safety agency.



5a. What are your thoughts about machine to machine data streams on the network?

Generally favorable and most concerns were about overuse of bandwidth and the regulation of overuse. Most were in favor of governmental/utility usage but not so agreeable to commercial usage on the NPSBN (burglar alarm companies, etc.)...(see table below).

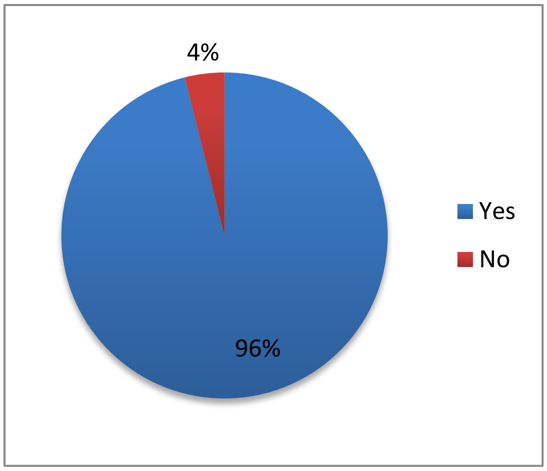
6. A State that chooses to manage its own infrastructure for the wireless data network independently of FirstNet can have a more, or less, restrictive definition of authorized network users compared to the national definition.



6a. What should happen if an eligible entity in one State responds to an incident in another state where the entity would not be considered eligible?

Generally agree that the entity, if authorized to respond, should be allowed on the network to perform duties for the requesting agency. (in many cases, predefined MOUs or IGAs were mentioned. In addition, there were strong feelings that there should be a consistent "user" base across all states to avoid this issue (see table below).

7. Should dispatchers, technicians and other personnel that support public safety qualify to use the FirstNet network?



Note: These questions were asked on two separate surveys with questions 1-4 having 94 respondents and questions 5-7 having 51 respondents.

What are your thoughts about machine to machine data streams on the network?	**What should happen if an eligible entity in one State responds to an incident in another state where the entity would not be considered eligible?**
Bio monitoring of responders, traffic cams and control, robots (flying and ground), hazmat monitoring, gunshot detectors, the list is endless.	Incident overrides could be allowed.
It would be especially good to know that our far-away repeater site for all our communications was down, and on generator backup, when it occurs via a communications signal of some sorts. This would allow for the Search and Rescue team to access our remote sits while there is still plenty of generator fuel, and not when it runs out and our transceivers go down.	They should of course be allowed - like a cross-certification standard as in other fields like emergency ingress and egress specialists, fire suppression, etc.
Although these would probably require only a small amount of space on the network at first, they are not true EMERGENCY responses and would eventually take up a lot of space. Where would you draw the line?	The State in which the entity is not eligible should be permitted to define the parameters for their jurisdiction, which is based on geography.
No routine burglar alarms but government DHS sensors yes. Telemetry for Paramedics yes.	Allow access
How old you regulate	We need to be nor the same rules
No thoughts on this matter	In today's age of interoperability that should not happen
Sounds like a good idea to ensure those devices continue to operate during an emergency.	They should be allowed based on the rules in their own state.
I feel that alarms should not be included. This is something that should be handled by an alarm company who is being paid for this service. Public water systems are a public safety issue and are typically handled by city government not be a business so they should be involved.	There needs to be interstate agreements that cover this. Much the same as when a police agency or fire agency assist another department out of their jurisdiction. They can not respond without a request and are governed by the rules of the home state in addition to following the rules of the state they respond in on.
	standardization criteria that follows the prescribed standards similar to the ones found within the wildland fire community- National Wildfire Coordinating Group- NWCG Standards based upon NIMS.

What are your thoughts about machine to machine data streams on the network?	**What should happen if an eligible entity in one State responds to an incident in another state where the entity would not be considered eligible?**
The network should have the ability to manage bandwidth in real time based on user priority. The rules should be established to provide minimum speeds/bandwidth to users in descending order of priority.	Similar to NIFOG interoperability radio channels, a guest network could be established and only activated during large incidents which require outside aid.
I think these types of tools are crucial	They should be considered eligible
Should be allowed as long as some limitation is applied to bandwidth usage .	YES
None.	
It drives the IT people nuts. With all of the "Hackers" attacking the US on every front, the less you allow to enter your network is probably best, but not very productive.	If you just look at Arizona, it seems to most of us that no one in the greater Phoenix area could care less about the rest of the state. I know that whenever we attend meetings in Maricopa County it like we just landed from Mars.
Because a machine is not provided by a public safety agency does not mean it should not be monitored by a public safety agency for security reasons and for emergency situations.	This entity should have the ability to handle emergencies and to assist FirstNet when emergencies arise, but have a channel or network address that is approved by FirstNet to assist.
I beleive that if they support critical infrastructure that they should be included.	There would need to be reciprocal clauses in the rules to recognize an entity recognized in another state in the event of an emergency.
Will it load the system and slow it down, does this data impact critical functions? It would say no, but then again, I think it is slowing thisprocess down.	This could create the same issues that started this entire issue of no interoperable communications. What will be done on the state boarders when there is an issue? I understand there might be cache handed out when needed, but on Initial Attack they will not be useful.

What are your thoughts about machine to machine data streams on the network?	What should happen if an eligible entity in one State responds to an incident in another state where the entity would not be considered eligible?
These data streams are extremely important and can be managed in such a way as to not cause interference with regular public safety communications. One example is electric, water and/or gas Utility Distribution Automation equipment that requires very low data rates but in the electric case, allows instantaneous switching and re-routing of critical circuits to prevent further damage and protect life and property in an area affected by any form of disaster. These functions on an electricity distribution system can effectively isolate an area before the first responders get there, greatly enhancing their own safety. Utilities have recently concluded that a minimum guaranteed bit rate of 250 Kbps on a per sector basis would be sufficient for this type of critical function. If Public Safety pre-emption could be done in such a way that utilities could keep this minimum bit rate open for critical functionality, then utilities would probably be able to participate in the PSBN. Other utility uses would be able to share the bandwidth with full pre-emption at any time by Public Safety. If utilities can obtain this small amount (less than 1% of the available LTE bandwidth)of guaranteed minimum bit rate (GBR)then PSBN participation, including negotiated access to utility telecom assets is possible.	If a utility were in this mode, reciprocity should be available at the time the service is being rendered. Under normal circumstances, the utility in this case should not be allowed to use the states' networks where it is not allowed however. It only makes sense that if Public Safety-related services are being performed in a critical emergency situation, then utilities need that ability if only for the duration of the crisis.
Network resources should be restricted to Public Safety agencies.	A "National" network should not differentiate agencies from another state from the local entities. If the required criteria is met by an agency to use the network, then it should apply nationwide.
There is a possibility that this could be taken advantage of. Even though it is possible to connect the data, not all data needs to be connected. This would cause excessive traffic on the network and addition time to process all the data that could adversely effect the systems involved. Data should be connected only if that connection has significant advantages over the current monitoring and notifications in place.	As the data format is the same across states, the entity should be allowed into the incident states system as if it is from the responding states system. All entities from one state should be able to be entered into another states system.

What are your thoughts about machine to machine data streams on the network?	**What should happen if an eligible entity in one State responds to an incident in another state where the entity would not be considered eligible?**
Perfectly fine with it!	The entity should be considered eligible.
They need to be completely owned and operated by a public safety agency or else they should be defined as commercial in nature and not acceptable traffic for First Net. Anything Not owned and operated by the government can use the carriers for back haul.	There needs to be a roaming agreement where those units that do not meet the criteria as eligible are grouped in to a lower priority pool of access, so if the hosting state runs short of resources the roaming ineligible units are moved to non First Net carriers until the sufficient resources become available.
Excellent resource, IF the access is properly protected.	User access should be controlled by the State.
Useful and can provide early alert. It is best that it goes out over a wired network to reduce cost and that test that the device is on-line occur daily or have alerts that the connection is down. Potentially too many devices for wireless.	
If it is mission critical and necessary for the safety of the public/community then it possibly should be allowed.	Does choosing to manage include paying independently or still using federal funds? I would think knowing you are responding to assist an ineligible state may change the rules as you should be accepting the rules as they apply to the location.
Use of data steams is a significant benefit to the system.	I would assume that the system would not identify the radio until after it is cleared through the Com-L for the incident
It should depend on who/what agency operates the machines collecting and receiving the data. Even though the machine is streaming the information without user interaction, it still means that a user could get on that machine to access the data network. Unless the data is absolutely critical to the public safety function, I would suggest that those streams come in via normal broadband sources.	Then the state in need that would be the beneficiary of the eligible entity from State number one wouldn't be able to receive that support, unless they make allowances for the eligible entity.
I would like to see this capability eventually but based on the current goals and configuration I believe this traffic would swamp the network for more important things.	A nation Authentication system needs to be in place for all devices, users and resources. Use in another region would have limited resources based on their national rights.
It would depend on the function of the data stream. Some functions of this would seem beneficial to be on the network.	Perhaps such instances should be handled before hand through the use of IGA's?

What are your thoughts about machine to machine data streams on the network?	What should happen if an eligible entity in one State responds to an incident in another state where the entity would not be considered eligible?
I think the potential for this to be misused because of loose interpretation as to what is critical is too possible.	If they are recognized in one state they should be recognized in all states. That is why I strongly disagree that each state should be allowed to make their own standards for a nation-wide system.
Machine to machine data Streams would be beneficial to the tribe.	It would not benefit the situation at all, it would probably slow the response protocol.
I guess it could be advisable. It would not be that much overhead, but security would have to be installed on each machine and it would have to be monitored at least periodically.	They would have to use the equipment of the state they are going to if they would be considered ineligible in that state or they could develop agreements or temporary authorizations with the state they are going to. Or, they could prepare to bring their own connectivity with them.
I don't believe that every alarm company should be able to send information over the network, but radiation leakage or high risk for terrorism, such as burglary of a building with radioactive materials, etc. should be considered a priority and allowed access to the system.	This should be covered by MOUs.
I think the priorities should be those data streams that detect criminal activity and conditions immediately dangerous to life and health. If the system can handle other relevant data streams that would not slow the system, that is fine.	The state wherein the incident is occurring has control. If there exists a method to allow temporary access and the controlling state grants permission in furtherance of the mission, then the entity has access, if that can be accomplished.
if clearly defined with a public safety purpose	They should retain privileges they roll with during a response
Alarm data brought in to our communications center in a timely manner would reduce the time of response.	Mismatched standards and expectations.
If the machine to machine data stream is used to support public safety is should be eligible to be on the First Net Network	It is incumbent on the responding agency to make sure they have the needed coverage.
It's important to transfer information between any kind of device that is authorized to operate on the network. From Mobile computers, to desktops to hand held devices.	The responding agency should be granted eligibility
Station security camera	

What are your thoughts about machine to machine data streams on the network?	**What should happen if an eligible entity in one State responds to an incident in another state where the entity would not be considered eligible?**
I can see where some devices ("things") may need to access the network during an incident for use by the incident responders. These would be deployed during the incident and removed afterwards. But I don't necessarily feel that devices operated by a non-public safety agency should run on the network because then where does it stop? Everyone will attempt to make a case to be on the network.	I think it needs to stay consistent otherwise there will be issues.
	Eligible entities within a state should only be allowed to respond to incidents within that state and/or other states in which they are eligible.
Alarm and sensors for fire, smoke or activation of fire suppression systems. Encrypted live streaming video able to be used as information to the Incident Command Post/ Emergency Operations Center. May also be utilized for emergency medical incidents where a physician has direct visualization of patient condition.	The entity representative will report to the Incident Command Post/ Emergency Operations Center or other identified area to participate in a unified command structure as recommended by NIMS and the National Response Framework document.
Machine to machine data should have a lower priority. Also it's gonna be hard to tell what data is from a "machine" and what data is initiated by a human.	Guess the receiving state can change their policy or 'demob' them from the incident.
	When an entity responds to an incident outside the state upon a "resource order" request through the requesting state's or the Federal Government's authority which should allow the entity to become eligible. If there is such a conflict, then a national standard should be established so that all entities would not encounter the situation the question asks.

What are your thoughts about machine to machine data streams on the network?	**What should happen if an eligible entity in one State responds to an incident in another state where the entity would not be considered eligible?**
Inasmuch as they support life safety they should be allowed, I can't imagine such systems putting a large load on the network…	Uniformity between states would be ideal, however it seems that they should be able to be granted access on an emergency basis. That would open up another issue of how to grant access quickly in an emergency and who is authorized to do it...
They should be sending to a dispatch on their own as what happens now. Too many potential users will clutter the system should a number of them need to use them all at once	That is why it should not be allowed to be different in various states.
As long as the machines are taught to notify a human element somewhere along the line.	Prior accreditation would help smooth the transition process.
Could be allowed but should be clearly defined and considered on case to case basis.	The definition of authorized network users should be the same and the interstate assistance should not be limited at the state level if allowed at the national level.
	Even if it is narrowed down there should be a provision for expanding it temporarily. For example special events, might need per event / incident flexibility to bring someone on temporarily.